PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-112494
(43)Date of publication of application : 23.04.1999

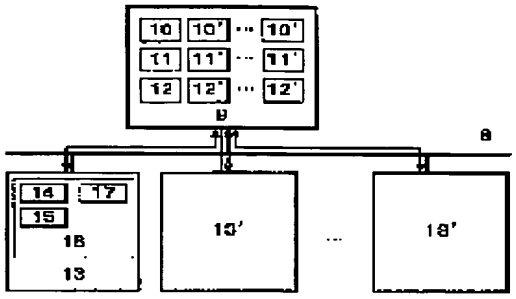
(51)Int.Cl. H04L 9/32
G06F 13/00
G09C 1/00
H04N 5/91
// H04N 7/167

(21)Application number : 09-271547
(22)Date of filing : 03.10.1997

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : YAMAGUCHI TOMOHISA

(54) CLIENT/SERVER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide high resistance against illegal copying by providing an illegal copying detect means for a client so as to detect illegal copying when illegal copying is tried in data cipher-released at the time of reproducing ciphered contents while dynamically releasing.
SOLUTION: At the client 13, a video reproducing application 16 executes an illegal copying detect module 17 and cipher releasing module 14. At the time of detecting illegal copying, the module 17 daises an illegal copying detect flag. Next, the application 16 checks the illegal copying detect flag. When the flag is raised, the execution of the module 14 is immediately finished and information on the detection of illegal copying is given to a video server 9. When the flag is not raised, ciphered video data 11 sent from the server 9 is cipher-released.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－112494

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７１
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ
// Ｈ０４Ｎ　7/167		7/167	Ｚ

審査請求　未請求　請求項の数11　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－271547

(22)出願日　平成９年(1997)10月３日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　山口　智久
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

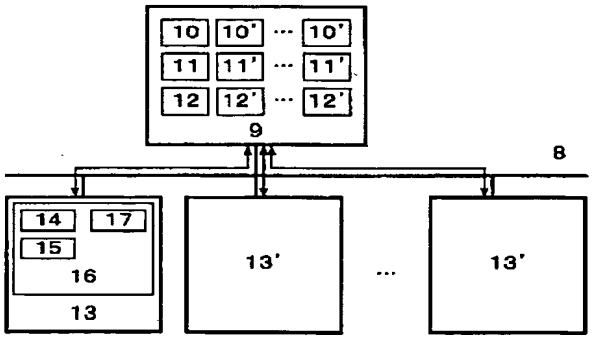
(74)代理人　弁理士　宮田　金雄　（外２名）

(54)【発明の名称】　クライアント・サーバシステム

(57)【要約】

【課題】　クライアントに不正コピー検出機能を設け、不正コピーに対して高い耐性を持たさせることを目的とする。

【解決手段】　ネットワークに接続されたサーバとクライアントからなるクライアント・サーバシステムにおいて、クライアントに不正コピー検出機能を設け、サーバから送られてくる暗号化コンテンツをクライアントで暗合を動的に解除しつつ再生する際において、暗合解除されたデータの不正コピーが試みられた場合に、不正コピー検出機能により不正コピーを検出し、不正コピーを防止するようにした。



【特許請求の範囲】
【請求項１】　ネットワークによって接続されたクライアント・サーバシステムにおいて、
クライアントはサーバから転送されてきた暗号化されたコンテンツを解除する暗号解除手段と、
不正コピー検出手段を備え、
該不正コピー検出手段は、暗号化されたコンテンツを上記暗号解除手段で動的に解除しつつ再生する際に暗号解除されたデータに不正コピーが試みられていた場合に、不正コピーを検出することを特徴とするクライアント・サーバシステム。
【請求項２】　上記不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、暗号解除を中止することを特徴とする請求項１記載のクライアント・サーバシステム。
【請求項３】　上記不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知することを特徴とする請求項１記載のクライアント・サーバシステム。
【請求項４】　上記不正コピー検出手段は、データに不正コピーが試みられたことを検出すると、不正コピーの内容とユーザ情報をサーバに通知することを特徴とする請求項１記載のクライアント・サーバシステム。
【請求項５】　サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止することを特徴とする請求項３または請求項４記載のクライアント・サーバシステム。
【請求項６】　ネットワークによって接続されたクライアント・サーバシステムにおいて、
サーバはビデオカメラから取り込んだビデオデータをリアルタイムにエンコードしながら暗号化を行う暗号化手段を備え、
クライアントはサーバから転送されてきた暗号化されたビデオデータを解除する暗号解除手段と、
不正コピー検出手段を備え、
該不正コピー検出手段は、サーバから送られてきた暗号化されたビデオデータを動的に暗合解除しつつ再生する際に、暗号解除されたビデオデータに不正コピーが試みられていた場合に、不正コピーを検出することを特徴とするクライアント・サーバシステム。
【請求項７】　上記不正コピー検出手段は不正コピーが試みられたことを検出した場合、暗号解除を中止することを特徴とする請求項６記載のクライアント・サーバシステム。
【請求項８】　上記不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知することを特徴とする請求項６記載のクライアント・サーバシステム。
【請求項９】　上記不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーの内容とユーザ情報をサーバに通知することを特徴とする請求項６記載のクライアント・サーバシステム。
【請求項１０】　サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止することを特徴とする請求項８または請求項９記載のクライアント・サーバシステム。
【請求項１１】　ネットワークによって接続されたクライアント・サーバシステムにおいて、
サーバはユーザ情報として暗号化コンテンツ利用権情報を保持し、
クライアントがコンテンツ利用権を有していないコンテンツにアクセスした場合、暗号化されたコンテンツの一部分に対応した暗号化されていない部分コンテンツを配信することを特徴とするクライアント・サーバシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はネットワークによって接続されたクライアント・サーバシステムで暗号化されたコンテンツの利用に関する。
【０００２】
【従来の技術】ネットワークによって接続されたクライアント・サーバシステムにおいて、サーバに格納されている暗号化されたコンテンツをクライアントで暗号を動的に解除しつつ、再生処理を行う従来システムにおける構成を図１１に示す。図１１において、１はネットワーク、２は暗号化コンテンツ（暗号化されたコンテンツ）をネットワーク１を通して配信するサーバ、３はサーバ２に格納されている暗号化コンテンツデータである。また、４はネットワーク１を通して暗号化コンテンツを受信するクライアント、５はサーバ２から送られてきた暗号化コンテンツデータの暗号解除を動的に行う暗号解除モジュール、６は暗号解除モジュール５で暗号解除した暗号化コンテンツデータのデコードを行うデコードモジュール、７は暗号化コンテンツの再生を行うコンテンツ再生アプリケーションである。
【０００３】サーバ２はクライアント４上のコンテンツ再生アプリケーション７からの配信要求により暗号化コンテンツデータ３をネットワーク１を通して配信する。コンテンツ再生アプリケーション７は、クライアント４に送られてきた暗号化コンテンツデータ３を暗号解除モジュール５、デコードモジュール６を使用して再生処理を行う。
【０００４】
【発明が解決しようとする課題】従来のクライアント・サーバシステムは、以上のようにして構成されていたので、暗合解除モジュール５で暗合解除した暗号化コンテ

ンツデータが、フック機能等を使用され、不正コピーされてしまう可能性があった。

【０００５】本発明は以上のような問題を解決するためになされたもので、クライアントに不正コピー検出機能を設け、不正コピーに対し高い耐性を有したクライアント・サーバシステムを提供することを目的とする。

【０００６】

【課題を解決するための手段】第１の発明は、ネットワークによって接続されたクライアント・サーバシステムにおいて、クライアントはサーバから転送されてきた暗号化されたコンテンツを解除する暗号解除手段と、不正コピー検出手段を備え、該不正コピー検出手段は、暗号化されたコンテンツを上記暗号解除手段で動的に解除しつつ再生する際に暗号解除されたデータに不正コピーが試みられていた場合に、不正コピーを検出するようにしたものである。

【０００７】第２の発明は、第１の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、暗号解除を中止するようにしたものである。

【０００８】第３の発明は、第１の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知するようにしたものである。

【０００９】第４の発明は、第１の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、不正コピーの内容とユーザ情報をサーバに通知するようにしたものである。

【００１０】第５の発明は、第３または第４の発明に係わるクライアント・サーバシステムにおいて、サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止するようにしたものである。

【００１１】第６の発明はネットワークによって接続されたクライアント・サーバシステムにおいて、サーバはビデオカメラから取り込んだビデオデータをリアルタイムにエンコードしながら暗号化を行う暗号化手段を備え、クライアントはサーバから転送されてきた暗号化されたビデオデータを解除する暗号解除手段と、不正コピー検出手段を備え、不正コピー検出手段は、サーバから送られてきた暗号化されたビデオデータを動的に暗合解除しつつ再生する際に、暗号解除されたビデオデータに不正コピーが試みられていた場合に、不正コピーを検出するようにしたものである。

【００１２】第７の発明は、第６の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は不正コピーが試みられたことを検出した場合、暗号解除を中止するようにしたものである。

【００１３】第８の発明は、第６の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知するようにしたものである。

【００１４】第９の発明は、第６の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーの内容とユーザ情報をサーバに通知するようにしたものである。

【００１５】第１０の発明は、第８または第９の発明に係わるクライアント・サーバシステムにおいて、サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止するようにしたものである。

【００１６】第１１の発明はネットワークによって接続されたクライアント・サーバシステムにおいて、サーバはユーザ情報として暗号化コンテンツ利用権情報を保持し、クライアントがコンテンツ利用権を有していないコンテンツにアクセスした場合、暗号化されたコンテンツの一部分に対応した暗号化されていない部分コンテンツを配信するようにしたものである。

【００１７】

【発明の実施の形態】

実施の形態１．本発明の第１の実施形態について、図１乃至図６に基づいて説明する。図１は本実施形態におけるシステム構成図であり、図において、８はネットワーク、９はネットワーク８を通して通常ビデオ（暗号化されていないビデオ）または暗号化ビデオ（暗号化されたビデオ）を配信するビデオサーバ、１０はユーザ情報、１１は通常ビデオデータ、１２は暗号化ビデオデータである。また、１３はネットワーク８を通して通常ビデオまたは暗号化ビデオを受信するクライアント、１４はビデオサーバ９から送られてきた暗号化ビデオデータの暗号解除を行う暗号解除モジュール、１５はビデオサーバ９から送られてきた通常ビデオデータまたは暗号解除モジュール１４で暗号解除したビデオデータのデコードを行うデコードモジュール、１６はユーザ認証、鍵交換、ビデオ再生等を行うビデオ再生アプリケーション、１７は暗号化ビデオの不正コピーの検出を行う不正コピー検出モジュールである。本実施形態ではコンテンツとしてビデオを扱っているが、オーディオ、動画、静止画、その他のコンテンツにも適用可能である。

【００１８】次に動作について図２、図３、図４を用いて説明する。ここで、図２はビデオ再生処理のフローチャートを示し、図３、図４は各々、ビデオ再生処理のフローチャート中における鍵交換処理（ステップ１３）、および暗号化ビデオ再生処理（ステップ１４）の詳細フ

ローチャートを示したものである。

【００１９】図２のビデオ再生処理フローチャートにおいて、まずビデオ再生アプリケーション１６はユーザが本システムを利用出来るか否かの認証を行うために、ログインダイアログボックスを出し、ユーザ名とパスワードを入力させ、これをビデオサーバ９に送る（ステップ１）。ビデオサーバ９では登録してあるユーザ情報を使用し、送られてきたユーザ名とパスワードからユーザ認証を行い、結果を返す。クライアント１３ではログインできた場合に限り（ステップ２）、以下の処理を実行することが出来る。次にビデオ再生アプリケーション１６はユーザからの要求を待ち（ステップ３）、ビデオ再生要求があった場合（ステップ５）には、ビデオサーバ９にビデオのタイトル情報を要求する。ビデオサーバ９はクライアント１３からの要求に従いビデオのタイトル情報を返す。ビデオ再生アプリケーション１６は送られてきたビデオのタイトル情報より、ビデオサーバ９に格納されているビデオの一覧を表示し、ビデオ選択ダイアログボックスを出し、ユーザにビデオを選択させる（ステップ６）。本実施形態では説明を簡素化するために、ユーザからの要求はビデオ再生要求とビデオ再生終了要求およびアプリケーション終了要求のみについて記述する。次に選択されたビデオの情報をビデオサーバ９に問い合わせ、選択されたビデオが暗号化されているかをチェックする（ステップ７）。暗号化されていない場合は、通常通りにビデオ再生を行う（ステップ８、ステップ９）。一方暗号化されている場合はユーザ情報１０をビデオサーバ９に問い合わせ、ユーザに暗号化ビデオ利用権利があるか否かをチェックする（ステップ１０）。

【００２０】ここで、ユーザ情報１０の構造を図５に示す。ユーザ情報１０はユーザ名、パスワード、暗号化ビデオ利用権利情報からなる。暗号化ビデオ利用権利情報には暗号化ビデオを利用できるか否かのみを示す情報を格納してもよいし、ビデオ毎に利用できるユーザのレベルを設定しておき、暗号化ビデオ利用権利情報にレベルを格納しておき、それを元に利用できるか否かの判定を行ってもよい。また、暗号化ビデオ利用権利情報にどのビデオを利用できるか、という情報を格納しておいてもよい。

【００２１】暗号化ビデオ利用権利がない場合（ステップ１１）、ビデオ再生アプリケーション１６は再生できない旨を表示して、ビデオの再生を行わず、ユーザからの要求待ち状態に戻ってもよいし、また可能であればビデオの先頭の数秒間などの暗号化ビデオに対応する部分再生をしてもよい（ステップ１２）。

【００２２】図６に部分再生を行う場合のビデオの格納方法を示す。暗号化ビデオデータに対応する部分データは暗号化されていないので、通常に再生を行うことができ、鍵交換を行う必要もない。ここでは部分データは暗号化ビデオデータの実ファイル名の一部を変換したものを例として挙げたが、別ディレクトリの同一ファイル名を使用するなど他の方法を用いてもよい。

【００２３】一方、暗号化ビデオ利用権利がある場合は、鍵交換処理を行う（ステップ１３）。鍵交換処理のフローチャートを図３に示す。本実施形態では共通鍵、公開鍵、秘密鍵を使用し鍵交換処理を行う。これは一例であり、他の鍵交換方式を使用することも出来る。暗号化ビデオの暗号化は共通鍵を使用している。図３において、まずビデオ再生アプリケーション１６は公開鍵と秘密鍵の生成を行う（ステップ３１）。次にユーザ情報と生成された公開鍵をビデオサーバ９に送る（ステップ３２）。一方、ビデオサーバ９は受け取ったユーザ情報から、再度ユーザ認証を行う（暗号化ビデオ利用権利もチェック）（ステップ２２）。ユーザ認証に成功した場合（ステップ２３）は受け取った公開鍵で暗号化ビデオの共通鍵を暗号化し（ステップ２４）、ビデオ再生アプリケーション１６に送る（ステップ２５）。　次にビデオ再生アプリケーション１６は、ビデオサーバ９から送られてきた公開鍵で暗号化された共通鍵を秘密鍵で暗号解除し、鍵交換処理を終了する（ステップ３４）。

【００２４】次にビデオ再生アプリケーション１６は暗号化ビデオ再生処理を行う。暗号化ビデオ再生処理のフローチャートを図４に示す。まずビデオ再生アプリケーション１６は暗号解除を行う前に不正コピー検出モジュール１７および暗号解除モジュール１４を実行させる（ステップ４１、ステップ４２）。不正コピー検出モジュール１７はビデオ再生アプリケーション１６の別スレッドとして動作し、実行を終了するまで常に不正コピーの検出を行い（ステップ４３）、もし不正コピーを検出した場合（ステップ４４）には不正コピー検出フラグを立てる。不正コピーの検出方法は、関数のアドレスをチェックしたり、Ｉ／Ｏを監視することなどがあげられるが、他の方法を用いてもよい。次にビデオ再生アプリケーション１６は不正コピー検出フラグをチェックする。フラグが立っていた場合は直ちに暗号解除モジュール１４の実行を終了させ（ステップ４５）、ビデオサーバ９に対して不正コピー検出を通知して（ステップ４６）、終了する。一方フラグが立っていなかった場合には、ビデオサーバ９から送られてくる暗号化ビデオデータ１１の暗号解除を行う（ステップ４７）。次にこの暗号解除された暗号化ビデオデータ１１のデコードを行い（ステップ４８）、ビデオおよびオーディオの出力を行う（ステップ４９）。これをビデオが終了またはユーザからのビデオ再生終了要求があるまで繰り返し（ステップ５０）、暗号化ビデオの再生を行う。ビデオが終了した場合には直ちに暗号解除モジュール１４の実行を終了して（ステップ５１）、不要な不正コピーの機会をなくす。次にユーザからの要求を待ち、ビデオ再生要求があった場合には上記したようにビデオの再生を行い、アプリケーション終了要求があった場合にはビデオ再生アプリケ

ーション１６を終了する。以上のようにビデオ再生処理を行う。

【００２５】実施の形態２．次に本発明の第２の実施形態について、図７乃至図１０に基づいて説明する。図７は本実施形態におけるシステム構成図であり、図７おいて１８はネットワーク、１９はネットワーク１８を通して暗号化ライブビデオ（暗号化されたライブビデオ）を配信するビデオサーバ、２０はユーザ情報、２１はビデオカメラ、２２はビデオカメラ２１から入力されたライブビデオをリアルタイムにエンコードするエンコードモジュール、２３はエンコードモジュール２２でエンコードされたライブビデオデータを動的に暗号化する暗号化モジュールである。また、２４はネットワーク１８を通して暗号化ライブビデオを受信するクライアント、２５はビデオサーバ１９から送られてきた暗号化ライブビデオデータの暗号解除を行う暗号解除モジュール、２６は暗合解除モジュール２５で暗合解除したライブビデオデータのデコードを行うデコードモジュール、２７はユーザ認証、鍵交換、暗号化ライブビデオ再生等を行う暗号化ライブビデオ再生アプリケーション、２８は暗号化ライブビデオの不正コピーの検出を行う不正コピー検出モジュールである。本実施形態ではコンテンツとしてライブビデオを扱っているが、ライブオーディオ、サーバに格納されているビデオ、オーディオ、動画、静止画その他のコンテンツにも適用可能である。

【００２６】次に動作について、図８、図９を用いて説明する。図８はビデオサーバ１９における暗号化ライブビデオ配信処理のフローチャートであり、図８（b）は図８（a）の暗号化ライブビデオ配信処理（ステップ７５の詳細フローチャートである。また、図９はクライアント２４における暗号化ライブビデオ再生処理のフローチャートである。まず図８において、ビデオサーバ１９ではユーザ（クライアントのユーザではなく、サーバのユーザであり、管理者などである）からエンコード開始要求に従い（ステップ７２）、ビデオカメラ２１からのライブビデオデータをエンコードモジュール２２でリアルタイムにエンコードする（ステップ７３）。次に、このライブビデオデータを暗号化モジュール２３で動的に暗号化する（ステップ７４）。この状態でクライアントからの要求を待つ（ステップ８０）。

【００２７】一方、図９のクライアント２４では暗号化ライブビデオ再生アプリケーション２７がユーザが本システムを利用出来るかの認証を行うために、ログインダイアログボックスを出し、ユーザ名とパスワードを入力させ、これをビデオサーバ１９に送る（ステップ５９）。

【００２８】すると、図８のビデオサーバ１９では登録してあるユーザ情報２０を使用し、送られてきたユーザ名とパスワードからユーザ認証を行い（ステップ８１）、結果を返し、クライアントからの要求待ちにもどる（ステップ８０）。

【００２９】クライアント２４ではログインできた場合に限り（ステップ６０）、以下の処理を実行することが出来る。暗号化ライブビデオ再生アプリケーション２７はユーザからの要求を待ち（ステップ６１）、暗号化ライブビデオ再生要求があった場合には（ステップ６２）ビデオサーバ１９にユーザ情報２０をサーバに問い合わせ、サーバからのユーザ情報に基づいて（ステップ８２）、ユーザが暗号化ライブビデオ利用権利があるかをチェックする（ステップ６３）。

【００３０】ユーザ情報２０は実施形態１と同一のものを使用してもよいし、図１０に示すように別途暗号化ライブビデオ利用権情報を保持するようにしてもよい。

【００３１】暗号化ライブビデオ利用権利がない場合（ステップ６４）、暗号化ライブビデオ再生アプリケーション２７はライブビデオの再生が出来ない旨を表示して（ステップ６５）ライブビデオを再生せず、ユーザからの要求待ち状態に戻る。一方、暗号化ライブビデオ利用権利がある場合は鍵交換処理を行う（ステップ６６）。鍵交換処理は実施形態１と同様のものである（図３）。次にライブビデオ再生アプリケーション２７は暗号化ライブビデオ再生処理を行う（ステップ６７）。暗号化ライブビデオ再生処理は実施形態１と同様のものである（図４）。暗号化ライブビデオ再生処理の中で、不正コピーが試みられたことが不正コピー検出モジュール２８で検出され、ビデオサーバ１９に不正コピー検出通知があった場合（ステップ８３）、ビデオサーバ１９ではライブビデオのエンコード、暗号化、他のクライアントへの暗号化ライブビデオの配信は続行し、不正コピーが検出されたクライアントへの暗号化ライブビデオの配信のみを中止する。またマルチキャストで配信している場合には不正コピーが検出されたクライアントをメンバからはずすことによって配信を中止する（ステップ８４）。さらにビデオサーバ１９ではクライアントから送られてきたユーザ情報、不正コピーの情報を履歴情報などに追加し、不正コピーの解析を行う（ステップ８５）。以上のようにして、暗号化ライブビデオ再生／配信処理を行う。

【００３２】

【発明の効果】第１の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出できるようにしたので、サーバに格納されている暗号化されたコンテンツをクライアントで暗号化解除する際に不正コピーに対する高い耐性を保持することができるという効果がある。

【００３３】第２の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると、暗合解除を中止することができるようにしたので、サーバに格納されている暗号化コンテンツをクライアントで暗号化解除する際に不正コピーをクライアント側か

ら防止できるという効果がある。

【００３４】第３の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出するとサーバに通知するようにしたので、サーバは格納されている暗号化コンテンツの配信を中止することができるという効果がある。

【００３５】第４の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると、ユーザ情報と不正コピーの内容をサーバに通知するようにしたので、不正コピーに対するフィードバックや不正コピーユーザに対する対応措置が可能となる。

【００３６】第５の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたり、不正コピーの内容とユーザ情報がサーバに通知されたときに、サーバはクライアントに対する暗号化コンテンツの配信を中止するようにしたので、不正コピーをサーバ側から防止できるという効果がある。

【００３７】第６の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出できるようにしたので、サーバが動的に暗号化したコンテンツをクライアントで暗号化を解除する際に不正コピーに対する高い耐性を保持することができるという効果がある。

【００３８】第７の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると暗合解除を中止するようにしたので、サーバが動的に暗号化したコンテンツをクライアントで暗号化解除する際に不正コピーをクライアント側から防止できという効果がある。

【００３９】第８の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことが直ちにサーバに通知されるので、サーバが動的に暗号化している暗号化コンテンツの配信を中止することができるという効果がある。

【００４０】第９の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると、ユーザ情報と不正コピーの内容をサーバに通知するようにしたので、不正コピーに対するフィードバックや不正コピーユーザに対する対応措置が可能となるという効果がある。

【００４１】第１０の発明に係わるクライアント・サーバシステムは、不正コピーが試みられるとサーバは動的に暗号化しているコンテンツの配信を中止するようにしたので、不正コピーをサーバ側から防止できるという効果がある。

【００４２】第１１の発明に係わるクライアント・サーバシステムは、サーバに暗号化コンテンツ利用権情報を保持し、該コンテンツに対する利用権を所持していないユーザに対しても、暗号化されたコンテンツの１部に対するアクセスを可能としたので、暗号化コンテンツの１部分を試聴することができるという効果がある。

【図面の簡単な説明】

【図１】　本発明の第１の実施形態を示すシステム構成図である。

【図２】　本発明の第１の実施形態におけるビデオ再生処理のフローチャートを示す図である。

【図３】　本発明の第１および第２の実施形態における鍵交換処理のフローチャートを示す図である。

【図４】　本発明の第１および第２の実施形態における暗号化ビデオ及びライブビデオ再生処理のフローチャートを示す図である。

【図５】　本発明の第１の実施形態におけるユーザ情報の構造を示す図である。

【図６】　本発明の第１の実施形態における暗号化ビデオに対応する部分データの格納方式を示す図である。

【図７】　本発明の第２の実施形態を示すシステム構成図である。

【図８】　本発明の第２の実施形態のビデオサーバにおける暗号化ライブビデオ配信処理のフローチャートである。

【図９】　本発明の第２の実施形態のクライアントにおける暗号化ライブビデオ再生処理のフローチャート示す図である。

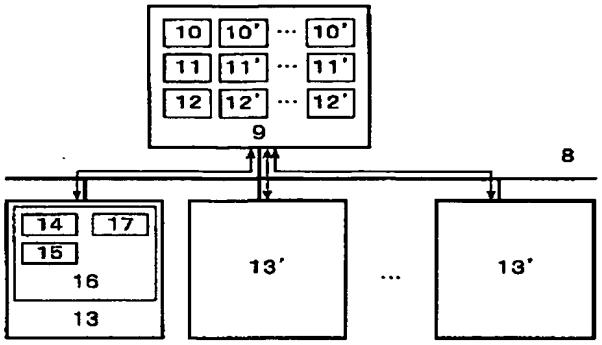
【図１０】本発明の第２の実施形態におけるユーザ情報の構造を示す図である。

【図１１】　従来の暗号化コンテンツを配信するクライアント・サーバシステム構成図である。

【符号の説明】

１　ネットワーク、２　サーバ、３　暗号化データ、４　クライアント、５　暗号解除モジュール、６　デコードモジュール、７　暗号化コンテンツ再生アプリケーション、８　ネットワーク、９　ビデオサーバ、１０　ユーザ情報、１１通常ビデオデータ、１２　暗号化ビデオデータ、１３　クライアント、１４　暗号解除モジュール、１５　デコードモジュール、１６　ビデオ再生アプリケーション、１７　不正コピー検出モジュール、１８　ネットワーク、１９　ビデオサーバ、２０　ユーザ情報、２１　ビデオカメラ、２２　エンコードモジュール２３　暗号化モジュール、２４　クライアント、２５　暗合解除モジュール、２６　デコードモジュール、２７　暗号化ライブビデオ再生アプリケーション、２８　不正コピー検出モジュール。

【図１】



【図５】

ユーザ情報
ユーザ名
パスワード
暗号化ビデオ利用権利情報

【図６】

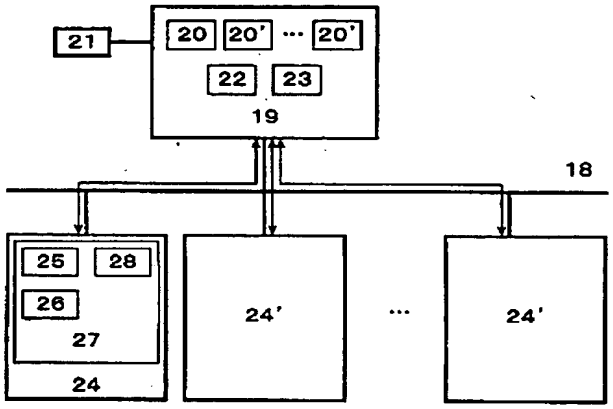
暗号化ビデオデータ

実ファイル名：xxxxxx.xxx

暗号化ビデオに対応する部分データ

実ファイル名：yxxxxxx.xxx

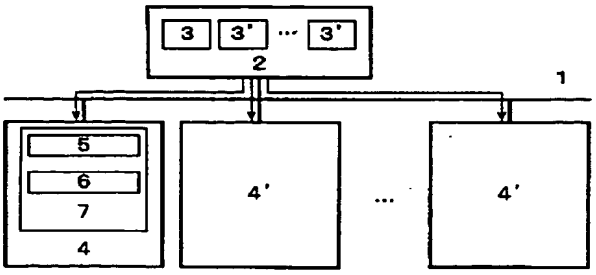
【図７】



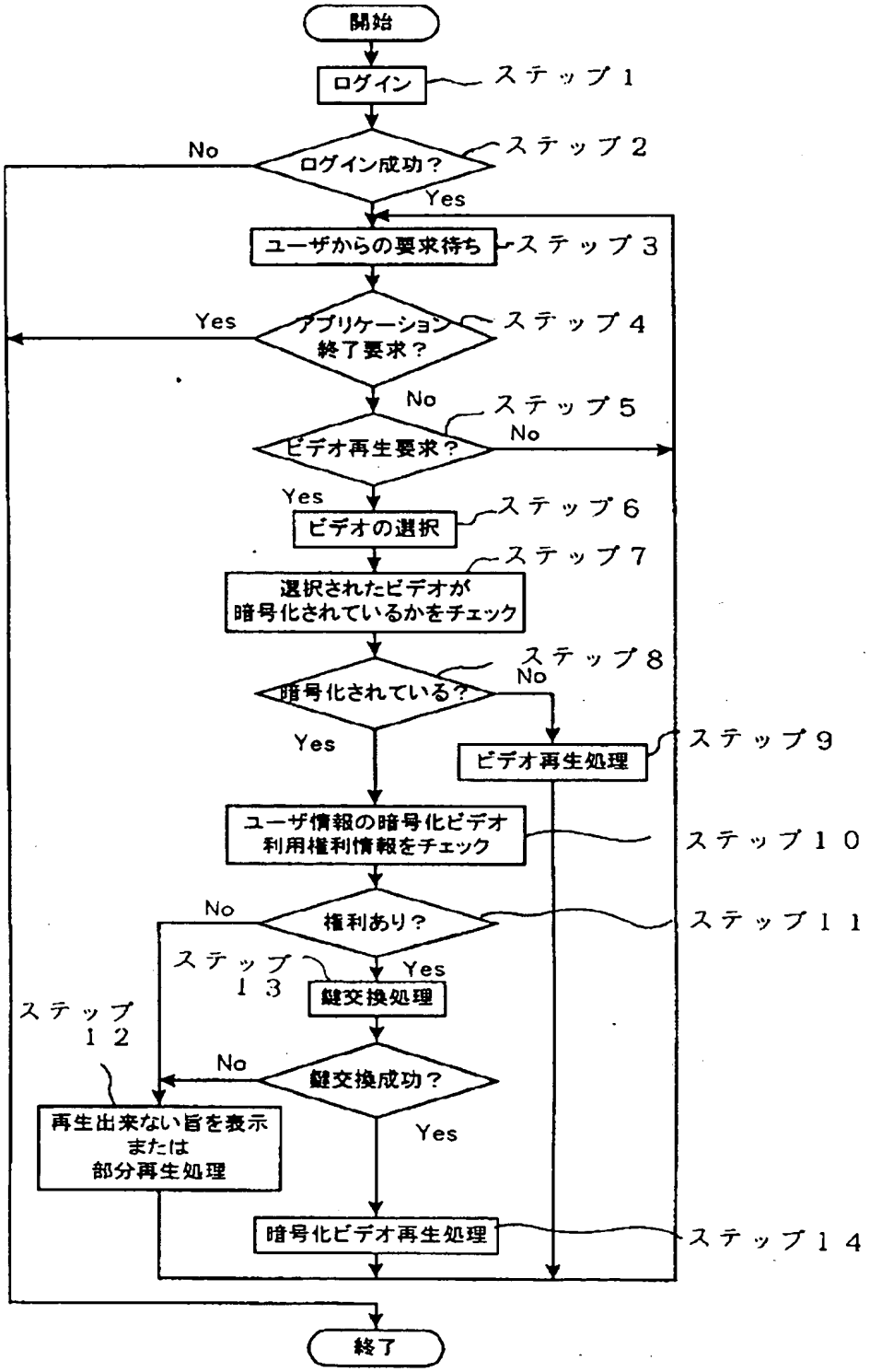
【図１０】

ユーザ情報
ユーザ名
パスワード
暗号化ビデオ利用権利情報
暗号化ライブビデオ利用権利情報

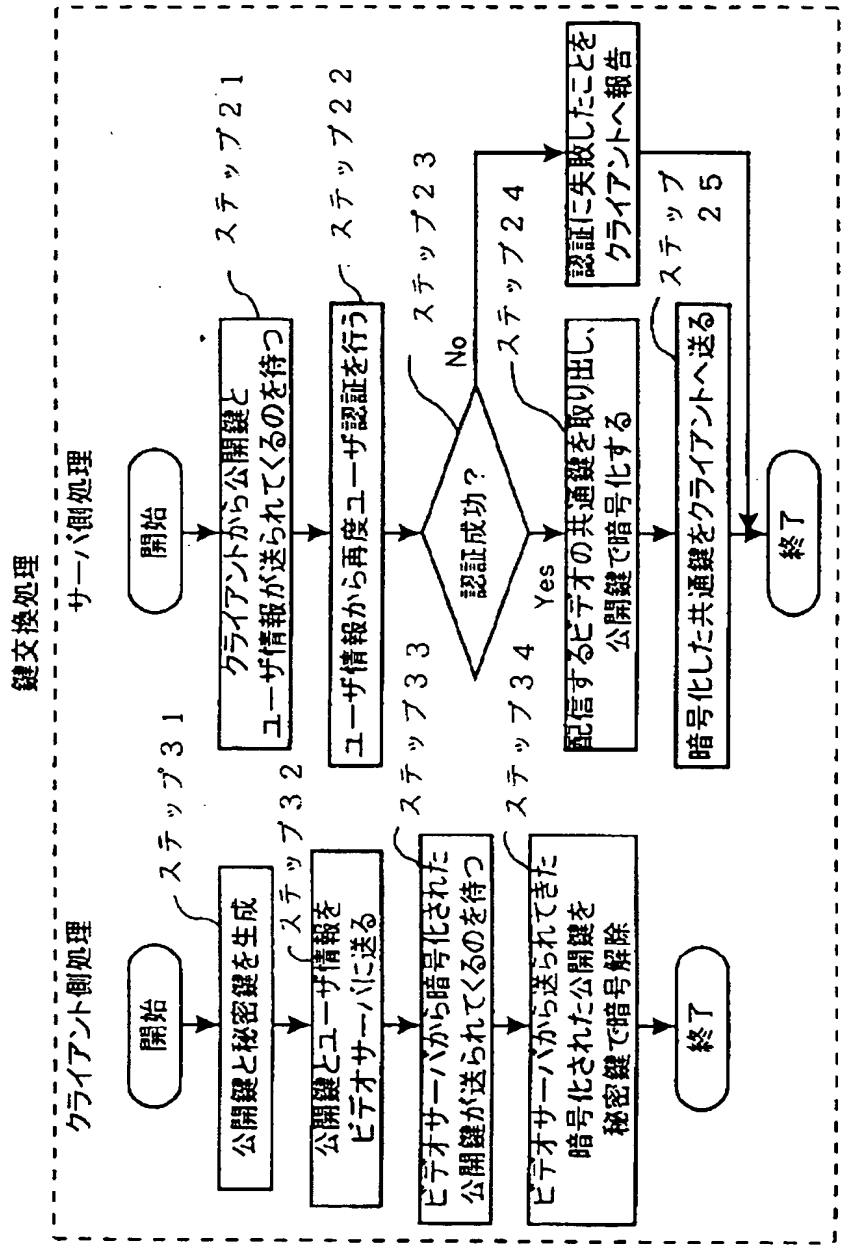
【図１１】



【図２】

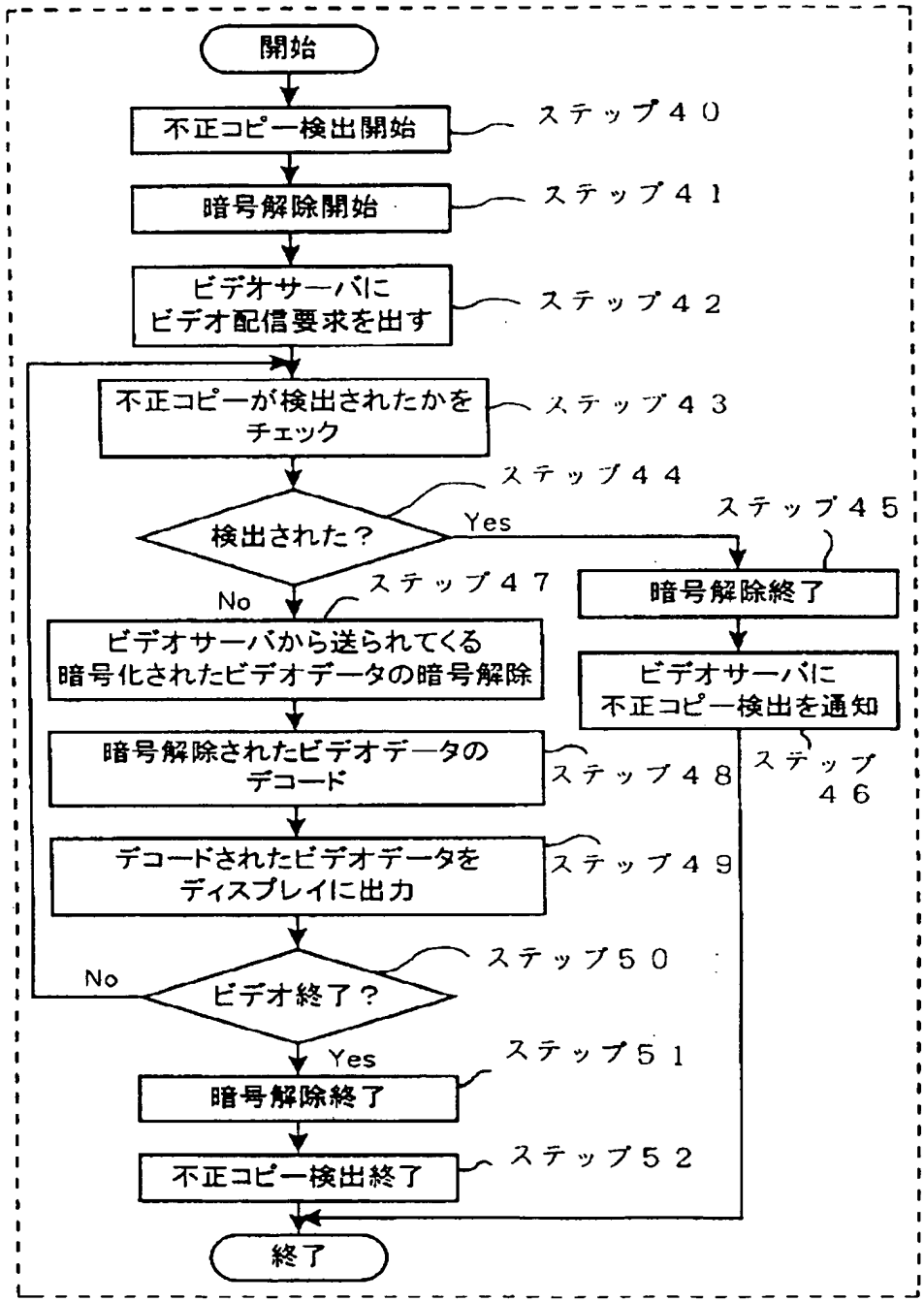

開始
ログイン
ステップ１
ログイン成功？
No
ステップ２
Yes
ユーザからの要求待ち
ステップ３
アプリケーション終了要求？
Yes
ステップ４
No
ビデオ再生要求？
ステップ５
No
Yes
ビデオの選択
ステップ６
選択されたビデオが暗号化されているかをチェック
ステップ７
暗号化されている？
ステップ８
No
Yes
ビデオ再生処理
ステップ９
ユーザ情報の暗号化ビデオ利用権利情報をチェック
ステップ１０
権利あり？
No
ステップ１１
ステップ１３
Yes
鍵交換処理
ステップ１２
No
鍵交換成功？
Yes
再生出来ない旨を表示または部分再生処理
暗号化ビデオ再生処理
ステップ１４
終了

【図３】

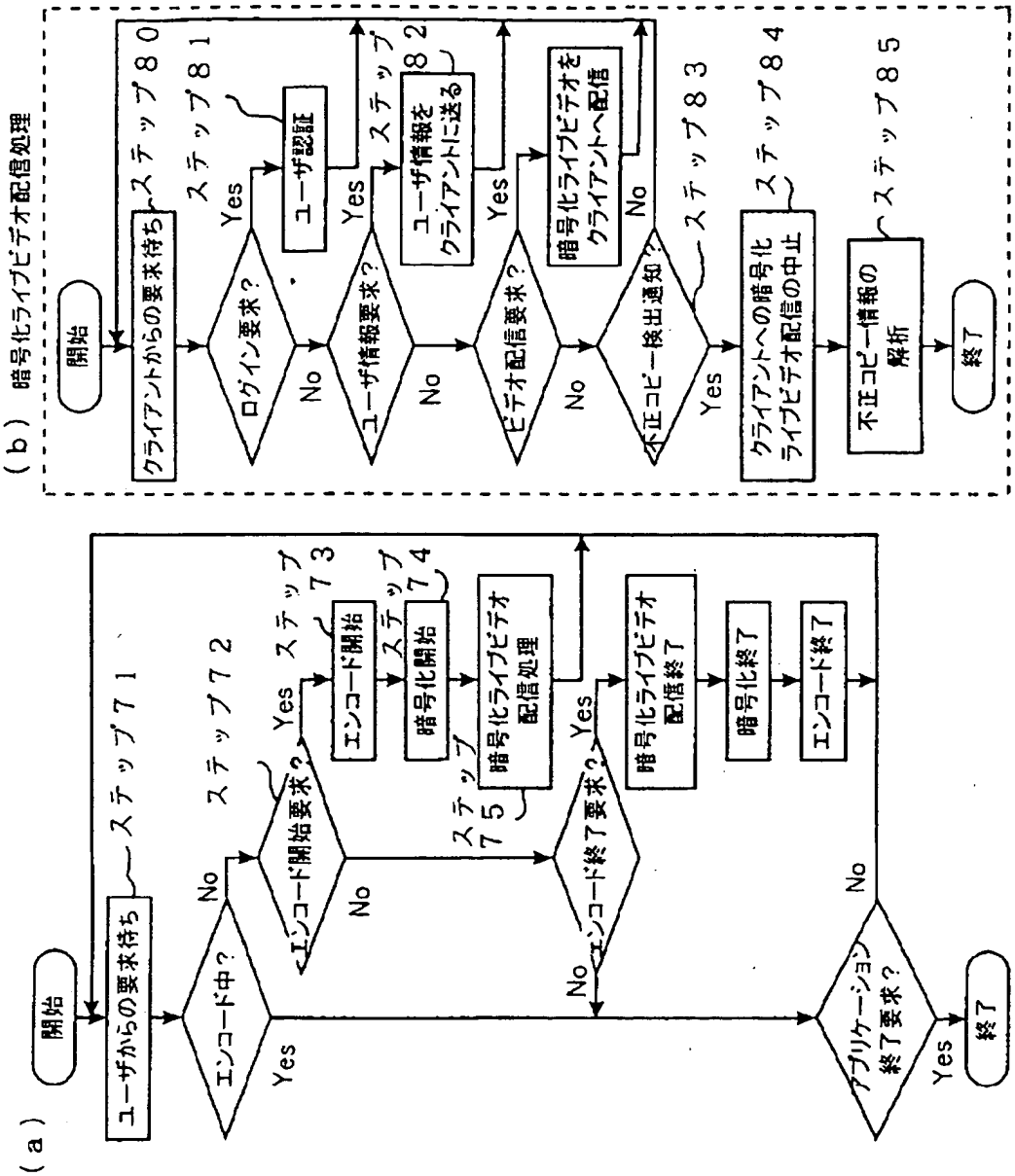

鍵交換処理
クライアント側処理
サーバ側処理
開始
ステップ３１
公開鍵と秘密鍵を生成
ステップ３２
公開鍵とユーザ情報をビデオサーバに送る
ステップ３３
ビデオサーバから暗号化された公開鍵が送られてくるのを待つ
ステップ３４
ビデオサーバから送られてきた暗号化された公開鍵を秘密鍵で暗号解除
終了
開始
ステップ２１
クライアントから公開鍵とユーザ情報が送られてくるのを待つ
ステップ２２
ユーザ情報から再度ユーザ認証を行う
ステップ２３
認証成功？
No
Yes
ステップ２４
配信するビデオの共通鍵を取り出し、公開鍵で暗号化する
認証に失敗したことをクライアントへ報告
ステップ２５
暗号化した共通鍵をクライアントへ送る
終了

【図４】

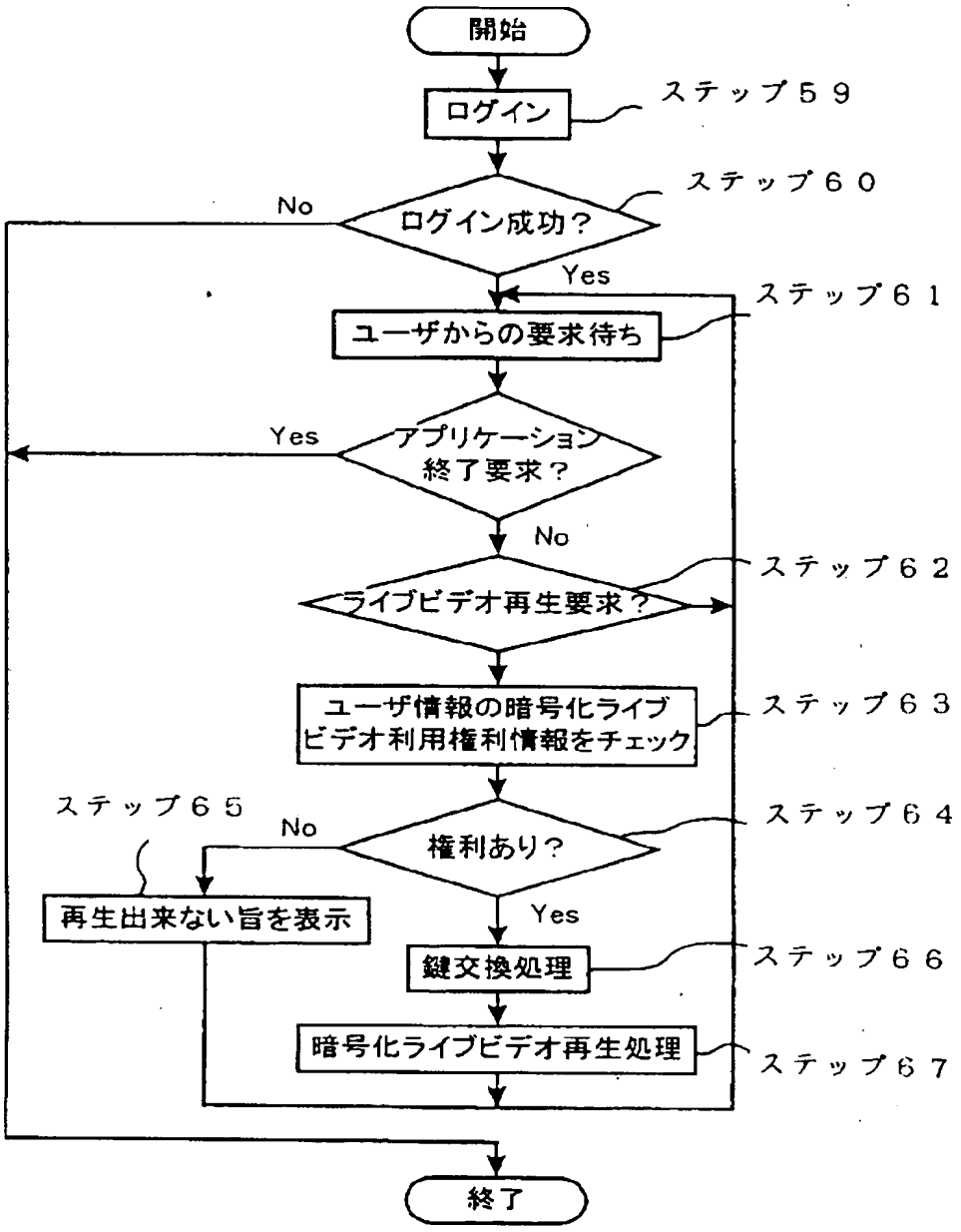
暗号化ビデオ／ライブビデオ再生処理



【図８】


(a)
開始
ユーザからの要求待ち
ステップ71
エンコード中？
No
Yes
ステップ72
エンコード開始要求？
No
Yes
ステップ73
エンコード開始
ステップ74
暗号化開始
ステップ75
暗号化ライブビデオ配信処理
エンコード終了要求？
No
Yes
暗号化ライブビデオ配信終了
暗号化終了
エンコード終了
アプリケーション終了要求？
No
Yes
終了
(b) 暗号化ライブビデオ配信処理
開始
クライアントからの要求待ち
ステップ80
ステップ81
ログイン要求？
Yes
No
ユーザ認証
ステップ82
ユーザ情報要求？
Yes
No
ユーザ情報をクライアントに送る
ビデオ配信要求？
Yes
No
暗号化ライブビデオをクライアントへ配信
不正コピー検出通知？
No
Yes
ステップ83
クライアントへの暗号化ライブビデオ配信の中止
ステップ84
不正コピー情報の解析
ステップ85
終了

【図９】


開始
ログイン
ステップ５９
ログイン成功？
ステップ６０
No
Yes
ユーザからの要求待ち
ステップ６１
アプリケーション終了要求？
Yes
No
ライブビデオ再生要求？
ステップ６２
ユーザ情報の暗号化ライブビデオ利用権利情報をチェック
ステップ６３
権利あり？
ステップ６４
ステップ６５
No
再生出来ない旨を表示
Yes
鍵交換処理
ステップ６６
暗号化ライブビデオ再生処理
ステップ６７
終了